UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AON RISK SERVICES NORTHEAST, INC.,

Plaintiff,

v.

MICHAEL KORNBLAU, TYLER WENDLEKEN, KARRYN ANGOFF, MARSH USA INC., MARSH & MCLENNAN COMPANIES, INC., and DOES 1-50, inclusive,

Defendants.

Case No. 10 CV 2244 (RMB) (JCF)

**PLAINTIFF'S MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS**

**TABLE OF CONTENTS**

**Page**

# TABLE OF AUTHORITIES

**Page**

**CASES**

## TABLE OF AUTHORITIES

**Page**

# TABLE OF AUTHORITIES

**Page**



**STATUTES**



**OTHER AUTHORITIES**

## I.
## PRELIMINARY STATEMENT

Aon Risk Services Northeast, Inc. ("Aon") is among many employers who "are increasingly taking advantage of the [Computer Fraud and Abuse Act]'s civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system." *Pac. Aero. & Electronics, Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003). The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA") originated as a criminal statute but "has been expanded over the last two decades." *P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC*, 428 F.3d 504, 510 (3rd Cir. 2005). In 1994, Congress amended the CFAA to authorize a private cause of action and "to expand the statute's scope to include civil claims challenging the unauthorized removal of information or programs from a company's computer database." *Pac. Aero.*, 295 F. Supp. 2d at 1196.

In the operative First Amended Complaint ("FAC"), Aon pleads a CFAA claim against three former employees, Michael Kornblau, Karryn Angoff, and Tyler Wendleken ("Former Employee Defendants"), and their new employer Marsh USA Inc. ("Marsh") (collectively, "Defendants"). The lawsuit alleges that together the Defendants conspired to and did abuse the limited computer access and usage rights Aon provided to the Former Employee Defendants, and wrongfully downloaded, accessed, altered, and deleted sensitive information and files contained therein. These allegations are contained in paragraphs 48 through 62 of the FAC, and together they detail the results of Aon's forensic investigation conducted on the Aon-issued computers of the Former Employee Defendants. That investigation revealed that, shortly before resigning, the Former

Employee Defendants attached 5 flash drives to Aon's computers and downloaded key information about the accounts they were currently servicing and deleted other information. This is a *prima facie* case under the CFAA which, as relevant here, provides a private right of action against a person (and his or her conspirator) who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer," 18 U.S.C. § 1030(a)(2)(C); or who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value…" 18 U.S.C. § 1030(a)(4).

Defendants seek dismissal of Aon's claim on the basis that the CFAA never reaches an employee who had permission to access his employer's computers. And this would be true, according to Defendants, regardless of whatever limitations (contractual or otherwise) were agreed to by the employee. Defendants argue that their reading of the CFAA is compelled by the plain terms of the statute, by the "overwhelming majority" of Courts (Defendants' Memorandum In Support of Their Motion To Dismiss Plaintiff's Complaint ("Opening Br.") at p. 4), and by rules of statutory construction and the legislative history of the CFAA.

But Defendants tell only half the story. There is a large body of conflicting law – even from cases within this circuit – that is likewise based on statutory interpretation principles and endorsed by Judge Posner in a published 7th Circuit decision, *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006). Contrary to the "narrow" construction of the CFAA proffered by Defendants, many courts apply the CFAA "broadly" and extend its protections to employers seeking federal recourse against

employees who hack computer files and breach their access rights just before walking out the door. Aon believes this Court will find the broader approach to be the correct one. But even under the narrow approach, the FAC here survives because that approach is concerned with allowing the CFAA to become a substitute for simple trade secret misappropriation but recognizes that the cause of action would still be available for acts of file deletion and alteration. The FAC here alleges acts of file deletion and alteration, not simply misuse of information.

Defendants also ask the Court to dismiss this lawsuit because Aon failed to plead a compensable "loss" under the CFAA. The CFAA makes its civil remedy available only to plaintiffs who expend at least $5,000 on such items as "the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense." 18 U.S.C. § 1030(e)(11). Aon alleges exactly that, namely, that it spent over $5,000 when it hired a consultant "to conduct a damage assessment and to restore any data or information that the Former Employee Defendants altered and/or deleted without authorization," and incurred "costs of investigating defendants' actions," among others. (FAC ¶¶ 48, 69.). Aon's federal claim should go forward.

## II.
## STATEMENT OF MATERIAL FACTUAL ALLEGATIONS

### A. Overview of Aon Trade Credit and Relationship to Defendants

Aon and its affiliated companies provide comprehensive insurance and risk management services across a wide variety of industries and through numerous product-lines. (FAC ¶ 14.) One such product-line is known as trade credit. Trade credit insurance, or trade credit services, offer niche products for typically large corporations

that seek unique insurance products such as insurance against account receivables filing bankruptcy, political risk insurance, and advice and services regarding credit control, bad debt protection, and international trade and investment. (FAC ¶¶ 15-16.) Aon provides these products through its Trade Credit Practice Group, within which highly trained insurance professionals including the Former Employee Defendants worked. (FAC ¶¶ 15-16, 24.)

As of the beginning of February 2010, Michael Kornblau was a Managing Director for the East Coast practice of Aon Trade Credit. (FAC ¶ 24.) Kornblau was responsible for managing and developing an Aon book of trade credit business, which he had done since joining Aon in 2001. (FAC ¶ 25.) Aon assigned other insurance professionals to assist Kornblau, including defendants Wendleken and Angoff. (FAC ¶ 24.)

**B. Aon Circumscribed and Limited the Former Employee Defendants' Computer Access Rights Through Promulgating Policies and By Requiring Kornblau and Angoff To Sign Employment Agreements.**

Aon depends upon maintaining the secrecy of a host of information, stored in paper or electronically, pertaining to its client and prospective client base and business plans, as well as information specific to in-force insurance-related programs. (FAC ¶¶ 20-21.) Such information includes, for instance, client lists, the identities and contact information of client decisionmakers, and premium and policy data unique to each client. Aon considers all such information to be confidential and trade secret, and takes numerous steps to limit its employees' usage and access rights of such information. (FAC ¶¶ 20-22.)

Those steps include, as alleged in paragraphs 22 and 37, "communicating policies to its employees that prohibit the use or disclosure of Aon trade secrets for non-business

purposes," "restricting access to offices which house such documents," password protecting computer access to only Aon employees, and permitting its employees to use such information "only for legitimate business purposes in the interest of Aon." (FAC ¶¶ 22, 37.)

It is also alleged that, "While they were employed by Aon, the Former Employee Defendants each had authority to access Aon's protected computers, databases, and software for the limited purpose of servicing existing business, or developing additional business, for the benefit of Aon, along with other incidental use necessary for their employment with Aon." (FAC ¶ 66.) Their access, however, was not "unfettered," as the Defendants suggest (Opening Br. at p. 1):

> While they were employed by Aon, the Former Employee Defendants were authorized to access their computers but only for a legitimate business purpose furthering Aon's interest and subject to the conditions of their employment. They were not authorized to improperly access, obtain, alter, and/or delete Aon confidential files and documents for the purpose of facilitating an unlawful solicitation of business or employees for the benefit of themselves or of an Aon competitor and to the detriment of Aon.

(FAC ¶ 67.)

Not only did Aon limit the Former Employee Defendants' computer access and usage rights by policy, Aon also required two of the defendants, Kornblau and Angoff, to sign employment agreements that contained materially identical non-disclosure provisions and that are attached to, and incorporated in, the First Amended Complaint. (FAC, Exs. A & B.) Both Kornblau and Angoff acknowledged that Aon possesses trade secrets and that they would "be granted otherwise prohibited access to such information." (FAC ¶¶ 26-28, Ex. A (Kornblau Agreement), § 6(a); FAC ¶¶ 32, 33; Ex. B. (Angoff Agreement) § 3(a).) They each agreed to the following non-disclosure provision:

> The Employee shall not, except as required in the course of employment hereunder, disclose or use during or subsequent to the course of employment, any Confidential Information which has not been publicly disclosed (other than by Employee in breach of this provision). All Confidential Information and all records and equipment and other materials relating in any way to Confidential Information shall be and remain the sole property of Aon Group during and after the end of employment.

(*Id.*)

**C. Defendants' Resignations and The Immediate Loss of Aon Business Prompted a Forensic Investigation Which Revealed Violations of the CFAA.**

The Former Employee Defendants all resigned from Aon during the first week of February 2010. (FAC ¶¶ 41-43.) Their resignations came as part of a conspiracy, led by Kornblau and Marsh executives, to raid Aon Trade Credit of its key trade credit clients and employees. (FAC ¶¶ 38-39.) Wendleken left first, on Tuesday, February 2nd. Then Angoff tendered her resignation on Wednesday, February 3rd. Kornblau left on Friday, February 5th. (FAC ¶¶ 41-43.) Immediately thereafter, Aon received a broker or record letter from a key client whose executive had met with Kornblau just three days earlier. (FAC ¶ 44.) The broker of record letter effected the appointment of the Former Employee Defendants' new employer, Marsh, as the new broker of record. It was effective on a date preceding two of their resignations. (*Id.*)

Their departures and the immediate loss of a large account prompted Aon to conduct a forensic investigation. (FAC ¶ 48.) Specifically, "Aon engaged Huron Consulting Group, Inc. to conduct a computer forensic analysis on the laptops assigned to the Former Employee Defendants . . . to conduct a damage assessment and to restore any data or information that the Former Employee Defendants altered and/or deleted without authorization." (FAC ¶ 48.)

The First Amended Complaint includes detailed factual allegations of the preliminary forensic findings, all of which provide factual evidence to support a *prima facie* CFAA claim:

**Kornblau's Computer Conduct**

- "Within the 10 days preceding Kornblau's resignation, ***he attached five portable computer storage devices and, in excess of his authorization, accessed documents that contained confidential and proprietary information***" such as client premium payments, detailed buying information, and annual policy program details. (FAC ¶ 51, emphasis added.)

- "On February 5, 2010, the day of his resignation, Kornblau ***altered a number of files from his computer, which he was not authorized to alter, including deleting*** contact files, budget reports, presentations, renewal reports, and other documents. Two of these files were labeled '2010 Budget,' and 'Contacts.'" (FAC ¶ 52, emphasis added.)

- "Kornblau also downloaded an 'Aon Commission Grid.' Aon Commission Grids show Aon's negotiated commissions for all lines of insurance globally for all markets. The secrecy of this information is extremely important as a broker's global commission information is not something that is easily ascertainable. It is highly competitive information. It is extremely unusual for a broker such as Kornblau to ever need to access such a document." (FAC ¶ 53.)

- "Kornblau also accessed an Aon internal network drive known as 'Aon Trade Credit' ***on 44 occasions in the month before his resignation. His frequent usage of this drive in the month before his departure was very unusual given that for over three***

***years preceding that time he did not access this location even once***." (FAC ¶ 54, emphasis added.)

**Angoff's Computer Conduct**

- "In the two weeks before her resignation, Angoff, in excess of her authorization, accessed more than 200 files containing confidential and proprietary information such as the premiums paid by Aon's global trade credit clients as well as multiple client files detailing buying information, annual policy program details and historical client transactions." (FAC ¶ 57.)

- "In this same time period, Angoff used her browser application to, in excess of her authorization, ***access files from the Aon Trade Credit network drive 239 times. In the previous one year period, she had accessed that same drive on just two occasions***." (FAC ¶ 58, emphasis added.)

- "On January 26, 2001, the same day she received her offer letter from Marsh, Angoff attached an external storage device to her computer. She accessed files containing Aon's proprietary information related to several Aon clients." (FAC ¶ 59.)

**Wendleken's Computer Conduct**

- "Between January 11 and February 2, 2010, Wendleken, in excess of his authorization, accessed approximately 76 Aon client-related files containing the confidential and proprietary information described above with respect to several Aon clients…." "Immediately prior to his resignation, Wendleken also, in excess of his authorization, accessed numerous files containing proprietary information of Aon, including client policy numbers, and invoices containing pricing." (FAC ¶ 61.)

This ongoing forensic analysis was not a free service, and the costs associated therewith and those incurred as a result are compensable under the CFAA, as set forth below. The First Amended Complaint pleads this specifically: Aon has incurred "losses well in excess of $5,000, which include, without limitation, the costs of investigating defendants' actions, assessing the resulting damages, restoring the data and information altered and/or deleted by the Former Employee Defendants, as well as the costs associated with the interruption to Aon's business[.]" (FAC ¶ 69.)

## III.
## ARGUMENT

### A. The First Amended Complaint Pleads a Cause of Action Under the CFAA.

To survive a motion to dismiss, Aon needs only to show that its claims are "plausible." *King Co., Wash. v. IKB Deutsche Industriebank AG*, Nos. 09 Civ. 8387(SAS), 09 Civ. 8822(SAS) , 2010 WL 1702196 at *2 (S.D.N.Y. Apr. 26, 2010). Dismissal is only appropriate where "it appears beyond doubt that the plaintiff can prove no set of facts in support of his claim which would entitle him to relief." *Conley v. Gibson*, 335 U.S. 41, 45-46, 78 S.Ct. 99 (1957). The allegations here clearly meet this standard.

The CFAA provides a civil right of action against a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C); § 1030(g) (expressly authorizing the maintenance of a civil action). And in subsection (a)(4), the CFAA provides a right of action against a person who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains

anything of value[.]" 18 U.S.C. § 1030(a)(4). Both of these provision include the phrases "without authorization" and "exceeds authorized access." The CFAA does not define the former, but it does define the latter: "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *Id.* § 1030(e)(6). The CFAA separately imposes civil liability on conspirators pursuant to 18 U.S.C. § 1030(b).

The First Amended Complaint pleads, under both subsections 1030(a)(2) and 1030(a)(4), that Defendants acted without authorization and in excess of their authority. The Former Employee Defendants each had a qualified right to access Aon's computer systems but only under certain conditions and for certain purposes. (FAC ¶¶ 22, 37, 66, 67.) Their access was circumscribed by Aon policies to which they were bound that prevented them from accessing Aon computer systems and files except in furtherance of legitimate business for the benefit of Aon. (*Id.*) In addition, two of the Former Employee Defendants, Kornblau and Angoff, had written agreements with Aon that likewise limited their rights to access and use Aon computers. (FAC ¶¶ 26-28, Ex. A (Kornblau Agreement), § 6(a); FAC ¶¶ 32, 33; Ex. B. (Angoff Agreement) § 3(a).) Those provisions included Kornblau and Angoff's non-disclosure agreements as well as their express acknowledgment that Aon possesses trade secrets and that they would "be granted otherwise prohibited access to such information." (FAC ¶¶ 26-28, Ex. A (Kornblau Agreement), § 6(a); FAC ¶¶ 32, 33; Ex. B. (Angoff Agreement) § 3(a).)

The First Amended Complaint alleges the preliminary results of a forensic investigation conducted on Aon's computer systems. (FAC ¶¶ 51-62.) That

investigation revealed several instances of file access, downloads, copying files to external thumb drive devices, file deletions, and highly irregular usage of unique files indicating foul play involving wrongful access of Aon computer files. (*Id.*; *see* section II(C), *supra*). It is further alleged that the Former Employee Defendants did so in conspiracy with Marsh "to exceed their legitimate access rights to Aon computers so that they could obtain, alter and/or delete Aon confidential and trade secret information for their own individual gain." (FAC ¶¶ 48-50.) Such conduct violated contractual obligations, violated fiduciary obligations and constituted trade secret misappropriation. The conduct also violated the CFAA.

**1. To The Extent The Language "Without Authorization" and "Exceeds Authorized Access" is Ambiguous, the CFAA Should Be Applied Broadly.**

**(a) Numerous Courts Follow A "Broad" Reading of the CFAA**

Judge Posner in a published 7th Circuit Court of Appeal decision articulated what is often referred to as the "broad" view of the CFAA. In *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006), Judge Posner reversed a dismissal of a CFAA claim against a former employee who deleted files and data from a company computer before quitting. Relying in part on the Restatement (Second) of Agency, Judge Posner held that an employee who breaches a duty of loyalty to an employer or acquires an adverse interest to her employer is no longer authorized to access the employer's computers and does so in violation of the CFAA. *Citrin*, 440 F.3d at 419-21. The Court explained:

> Citrin's breach of his duty of loyalty terminated his agency relationship (more precisely, terminated any rights he might have claimed as IAC's agent--he could not by unilaterally terminating any duties he owed his principal gain an advantage!) and with it his authority to access the laptop,

> because the only basis of his authority had been that relationship. "Violating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship." *State v. DiGiulio*, 172 Ariz. 156, 835 P.2d 488, 492 (App. 1992). "Unless otherwise agreed, the authority of the agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal." *Id.; Restatement, supra*, § 112[1]; see also *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, [119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000)]; cf. *Phansalkar v. Andersen Weinroth & Co.*, 344 F.3d 184, 201-02 (2d Cir. 2003) (per curiam); *Restatement, supra*, § 409(1) [2] and comment b[3] and illustration 2.

*Citrin*, 440 F.3d at 420-21.

Applying Restatement principles to interpret the phrase "authority" is consistent with federal law. As one district court recently explained when agreeing with Judge Posner's views, "Courts, acknowledging the importance of agency law in discussing 'authority,' have applied agency law to federal statutes to effect the statute's clear

---

[1] Restatement (Second) of Agency § 112, "Disloyalty of Agent," provides: "Unless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal."

[2] Restatement (Second) of Agency § 409(1) provides: "A principal is privileged to discharge before the time fixed by the contract of employment an agent who has committed such a violation of duty that his conduct constitutes a material breach of contract or who, without committing a violation of duty, fails to perform or reasonably appears to be unable to perform a material part of the promised service, because of physical or mental disability."

[3] Restatement (Second) of Agency § 409 comment b provides, *inter alia*: "Agents are appointed to forward the principal's interests, and when the agent ceases to do this and prefers his own or another's interests, ordinarily the principal no longer would desire the agent to act for him, and this the agent should realize. Whether or not the disloyalty of the agent is such that he should realize that the principal would desire the termination of his entire authority at once is a question of fact. Where the agent acquires an interest adverse to that of the principal or acts for another principal, and this is not known to the principal, ordinarily he should realize that the principal would not desire him to continue to act, although he does exactly what he would have done otherwise."

language and its intended purpose." *NCMIC Finance Corp. v. Artino*, 638 F. Supp. 2d 1042, 1057 (S.D. Iowa 2009) (citing *Faragher v. City of Boca Raton*, 524 U.S. 775, 803 n. 3, 118 S.Ct. 2275, 141 L.Ed.2d 662 (1998) (interpreting Title VII as requiring an employer's vicarious liability for its employees' sexual harassment because "our obligation here is not to make a pronouncement of agency law in general ... [but] adapt agency concepts to the practical objectives of Title VII"); *Commerford v. Olson*, 794 F.2d 1319, 1323 (8th Cir. 1986) (interpreting federal securities laws and finding that applying "common law agency principles to determine secondary liability for violations of the securities acts does not expose corporations, employers, and other such potential defendants to strict liability for all acts of their agents or cause them to be insurers of their agent's actions"); and *Citrin*).

*Citrin* and cases like it are alive and well in the 7th Circuit[4] and beyond. Several years before, the 1st Circuit ruled similarly in *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 62 (1st Cir. 2003), where it held that an employee breached his confidentiality agreement with his ex-employer by using confidential information he obtained as an

[4] *E.g.*, *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760, 767 (N.D. Ill. 2009) ("Allegations that an employee e-mailed and downloaded confidential information for an improper purpose are sufficient to state a claim that the employee exceeded her authorization [under the CFAA]."); *Dental Health Products, Inc. v. Ringo*, No. 08-C-1039, 2009 WL 1076883, *7 (E.D. Wis. Apr. 20, 2009) (allegation that defendant breached his duty of loyalty by going to work for one of its competitors while remaining in its employ is therefore sufficient to state a section 1030(g) claim that he violated section 1030(a)(2)"); *TEKsystems, Inc. v. Modis, Inc.* No. 08 C 5476, 2008 WL 5155720, *4-5 (N.D. Ill. Dec. 5, 2008); *Mintel Int'l Group, Ltd. v. Neergheen*, No. 08 C 3939, 2008 WL 2782818, *3 (N.D. Ill. July 16, 2008); *Forge Indus. Staffing, Inc. v. De La Fuente*, No. 06 C 3848, 2006 WL 2982139, *5-6 (N.D. Ill. Oct. 16, 2006); *C.H. Robinson Worldwide, Inc. v. Command Transp., LLC*, No. 05 C 3401, 2005 WL 3077998, at *2-4 (N.D. Ill. Nov. 16, 2005) (allegations that former employees continued to possess plaintiff's electronic files and data for their personal gain sufficient to establish CFAA claim).

employee to obtain information from his ex-employer's website thereby exceeding his authorized access in violation of the CFAA.[5] More recently, the 5th Circuit Court of Appeal held similarly in a criminal case under the CFAA. *United States v. John*, 597 F.3d 263, 270-73 (5th Cir. 2010) (upholding CFAA conviction where former employee misused his access to employer's computers to perpetrate a fraud in violation of employer's policies, stating "[a]ccess to a computer and data that can be obtained from that access may be exceeded if the purpose for which access has been given are exceeded"). Many other courts agree with Judge Posner's views, including courts in the 3rd Circuit,[6] the 5th Circuit,[7] the 8th Circuit,[8] and the 9th Circuit.[9]

---

[5] *See also Guest-Tek Interactive Entertainment, Inc. v. Pullen*, 665 F.Supp.2d 42, 44-46 (D. Mass. 2009) (CFAA claim upheld where former employee "surreptitiously transposed" his employer's computer files onto his personal USB device).

[6] *E.g. Dudick, ex rel. Susquehanna Precision, Inc. v. Vaccarro*, No. 3:06-CV-2175, 2007 WL 1847435, at *5 (M.D. Pa. June 25, 2007) (employer had stated CFAA claim when its employee accessed employer's proprietary information and used it to benefit a new employer); *Hub Group, Inc. v. Clancy*, No. Civ. A. 05-2046, 2006 WL 208684, at *4 (E.D. Pa. Jan. 25, 2006) (employee's breach of confidentiality provision equated to CFAA violation, following *Shurgard* cases).

[7] *E.g.*, *Hewlett-Packard Co. v. Byd:Sign, Inc.*, No. 6:05-CV456, 2007 WL 2755476 (E.D. Tex. Jan. 25, 2007) ("In contrast, HP has actually alleged that the Defendants had agreed not only to refrain from disclosing information, but also to refrain from sending or accessing messages on HP's computer systems for personal gain. By doing so, HP has alleged actual access without or in excess of authorization.")

[8] *E.g.*, *NCMIC Finance Corp. v. Artino*, 638 F.Supp.2d 1042 (S.D. Iowa 2009); *Lasco Foods, Inc. v. Hall and Shaw Sales, Marketing, & Consulting, LLC*, No. 4:08CV01683 JCH, 2009 WL 3523986, *2-4 (E.D. Mo. Oct. 26, 2009) ("Under the [CFAA], the Restatement, and the reasoning of *Citron* and other courts, Lasco sufficiently alleged that Hall and Shaw acted without authorization when they obtained Lasco's Information for their personal use and in contravention of their fiduciary duty to their employer, Lasco."); *Nilfisk-Advance, Inc. v. Mitchell*, No. Civ. 05-5179, 2006 WL 827073, *2 (W.D. Ark. March 28, 2006) (upholding CFAA claim where employee sent employer's computer files confidential information to himself with the intent to misappropriate trade secrets).

Likewise, there are several courts in this circuit which have taken a broader view of the CFAA. While Defendants have focused primarily on two cases which have taken a more narrow view of the statute (*Jet One Group, Inc. v. Halycon Jet Holdings, Inc.*, No. 08-CV-3980 (JS)(ETB), 2009 WL 2524864 (E.D.N.Y. Aug. 14, 2009); *Orbit One Communications, Inc. v. Numerex Corp.*, Nos. 08 CIV 0905(LAK), 08 CIV 6233(LAK), 08 CIV 11195(LAK), 2010 WL 847133 (S.D.N.Y. Mar. 10, 2010)), there are several cases which have permitted a CFAA claim in circumstances similar to those alleged here. In *Caylon v. Mizuho Securities USA, Inc.*, No. 07 CIV 2241 (RO), 2007 WL 2618658 (S.D.N.Y. Sept. 5, 2007), for example, a former employer sued several of its former employees and their new employer for violations of the CFAA and a number of state law claims including breach of fiduciary duty, inducing/aiding and abetting a breach of fiduciary duty, unfair competition, tortious interference and conspiracy. The plaintiff alleged that, before leaving, the former employees copied information from plaintiff's computers and emailed such records to their own personal email accounts and their new employer. Judge Kaplan denied defendants' motion to dismiss the complaint:

---

[9] *E.g.*, *Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc.*, 556 F. Supp. 2d 1122, 1131 (E.D. Cal. 2008) ("Employees that access their employer's computers to obtain or delete business information for their own personal benefit or the benefit of a competitor act 'without authorization' or 'exceed authorization' within the meaning of the [CFAA]."); *Pac. Aero. & Electronics, Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1194-97 (E.D. Wa. 2003) (allegations that former employee wrongfully obtained plaintiff's customer information and its technology sufficient to establish CFAA claim, examining history of CFAA and case law development); *ViChip Corp. v. Lee*, 438 F. Supp. 2d 1087, 100 (N.D. Cal. 2006) (executive who deleted information from company server and computer after he knew he was to be terminated violated the CFAA); *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (finding that employee acted without authorization when he obtained proprietary information from his employer's computers for the benefit of his new employer)

> Courts in other circuits have interpreted the "without authorization" and "exceeds authorized access" in different ways. But, the plain language of the statute seems to contemplate that, whatever else, "without access" and "exceeds authorized access" would include an employee who is accessing documents on a computer system which that employee had to know was in contravention of the wishes and interests of the employer. Accepting as true the allegations in the complaint, Caylon's employees did not have authorization to access the Caylon computer system and take out proprietary documents for use by a competitor bank. On that basis, Caylon has stated a claim under the CFAA, and there is federal jurisdiction.

*Caylon*, No. 07 CIV 2241 (RO), 2007 WL 2618658 at *1. *See also Modis, Inc. v. Bardelli*, 531 F. Supp. 2d 314, 317-19 (D. Conn. 2008) (finding plaintiff sufficiently pled the CFAA element of "access that exceeded authorization" where employee accessed information about plaintiff's clients for her own purposes); *Penrose Computer MarketGroup, Inc. v. Camin*, 682 F. Supp. 2d 202 (N.D.N.Y. 2010) (upholding CFAA claim against former employee); *The Dedalus Foundation v. Banach*, No. 09 Civ. 2842(LAP), 2009 WL 3398595 (S.D.N.Y. Oct. 16, 2009) (same).

**(b) CFAA Legislative History Supports the Broad Reading**

While Defendants base their legislative history analysis on 1986 Senate Reports (Opening Br. at 9 (expressly omitting citation to 1986 Senate reports)), many Courts rely on a more recent (by ten years) Senate Report relating to the 1996 amendment which broadened the statute by substituting the phrase "federal interest computer" with "protected computer." *E.g., Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1128-29 (W.D. Wash. 2000); *NCMIC Finance Corp. v. Artino*, 638 F. Supp. 2d 1042, 1058-59 (S.D. Iowa 2009). These cases rely on several excerpts of the Senate Report, which include:

- "[The CFAA is strengthened] by closing gaps in the law to protect better the confidentiality, integrity, and security of computer data and networks."

- "[The CFAA] facilitates addressing in a single statute the problem of computer crime, rather than identifying and amending every potentially applicable statute affected by advances in computer technology. As computers continue to proliferate in businesses and homes, and new forms of computer crimes emerge, Congress must remain vigilant to ensure that the [CFAA] is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime."

- "The proposed subsection 1030(a)(2)(C) is intended to protect against the interstate or foreign theft of information by computer.... This subsection would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected. In instances where the information stolen is also copyrighted, the theft may implicate certain rights under the copyright laws. The crux of the offense under subsection 1030(a)(2)*(C), however, is the abuse of a computer to obtain the information.*"

- "Those who improperly use computers to obtain other types of information-such as financial records, nonclassified Government information, and information of nominal value *from private individuals or companies* -face only misdemeanor penalties, *unless the information is used for commercial advantage,* private financial gain or to commit any criminal *or tortious act.*"

- "For example, individuals who intentionally break into, *or abuse their authority to use,* a computer and thereby obtain information of minimal value of $5,000 or less, would be subject to a misdemeanor penalty. The crime becomes a felony if the offense was committed for *purposes of commercial advantage* or private financial gain, for the purposes of *committing any criminal or tortious act in violation* ... of the laws of the United States or of any State, or if the value of the information obtained exceeds $5,000."

*Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d at 1128-29 (quoting S. Rep. No. 104-357 (1996) (emphasis in original)). The court in *Shurgard* reviewed this Senate Report and concluded that:

> This legislative history, although in reference § 1030(a)(2), demonstrates the broad meaning and intended scope of the terms "protected computer" and "without authorization" that are also used in the other relevant sections. The report recognizes that someone could be liable under § 1030(a)(2)(C) where intellectual property rights are involved. Finally, the report states the statute is

> intended to punish those who illegally use computers for commercial advantage. In sum, this passage makes clear that the CFAA was intended to encompass actions such as those allegedly undertaken by the present defendant. The legislative history of the CFAA comports with the plain meaning of the statute.

*Id.* at 1129. This Court should adopt similar reasoning.

**(c) The Rule of Lenity Does Not Bar This View**

Defendants also raise the rule of lenity, arguing that any ambiguity should be resolved in their favor given that the CFAA also has criminal applications. (Opening Br. at 9-12.) The Firth Circuit addressed this argument when affirming a criminal CFAA conviction in *United States v. John*, 597 F.3d 263 (5th Cir. 2010). There, the Court of Appeal explained that the rule of lenity need not apply where the defendant "has reason to know" that he or she "is not authorized to access data or information in furtherance of a criminally fraudulent scheme." *Id.* at 273. "[W]hen an employee knows that the purpose for which she is accessing information in a computer is both in violation of an employer's policies and is part of an illegal scheme, it would be 'proper' to conclude that such conduct 'exceeds authorized access' within the meaning of § 1030(a)(2)." *Id.*

Here, the defendants "had reason to know" they were violating company policy and, as to two of them, their employment agreements, not to mention breaching fiduciary obligations and committing trade secret misappropriation, among other things. Accordingly, these defendants knew or should have known their acts were wrongful, and the rule of lenity should not operate to preclude this claim.

In short, the First Amended Complaint properly pleads that the Former Employee Defendants exceeded their authorized access by improperly accessing, in excess of their authority, Aon computer files and systems in order to take Aon computer records and then "deleted electronic communications and files in an effort to cover their tracks and

prevent Aon from discovering their unlawful conspiracy and theft of Aon files and trade secret information." (FAC ¶ 49.) Such conduct supports claims under both subsection 1030(a)(2) and 1030(a)(4). Under subsection 1030(a)(2), Aon need only show intentional access "without or authorization or exceeds authorized access." Under subsection 1030(a)(4), Aon must show the same but, in addition, that the defendants (1) acted "with intent to defraud" and (2) obtained "anything of value." The Defendants' illicit intent is alleged throughout the First Amended Complaint (*e.g.*, FAC ¶ 38 (defendants conspiring "for the purpose of unlawfully soliciting Aon clients and employees"); FAC ¶ 44 ("the Defendants together and individually disclosed [Aon confidential information] to Marsh to facilitate Marsh's appointment as the broker of record for [an Aon] client"); FAC ¶ 49 ("the Former Employee Defendants deleted electronic communications and files in an effort to cover their tracks and prevent Aon from discovering their unlawful conspiracy and theft of Aon files and trade secret information").)

**2. Even Under Defendants' Narrow View of The CFAA, This Motion Should Be Denied.**

Defendants rely on the reasoning of several cases, including one from this district, (*Orbit One Communications, Inc. v. Numerex Corp.*, Nos. 08 CIV 0905(LAK), 08 CIV 6233(LAK), 08 CIV 11195(LAK), 2010 WL 847133 (S.D.N.Y. Mar. 10, 2010)), which hold that, contrary to agency principles followed by other federal courts, the CFAA should be narrowly interpreted so as not to apply to employees who misuse their lawful computer access. (Opening Br. at 4-6.) In *Orbit One Communications, Inc.*, Judge Kaplan dismissed a CFAA claim on summary judgment, where the plaintiff alleged that the defendants "intentionally accessed Numerex's computer system and downloaded

information contained on that system … for the purpose of competing with Numerex." *Orbit One Communications, Inc.*, 2010 WL 847133 at *8. On those allegations, Judge Kaplan granted the employee's summary judgment motion, refusing to extend CFAA coverage to mere trade secret misappropriation. "[The CFAA] as a whole indicates Congress's intent to prohibit access of a computer without authorization, not an employee's misuse of information that he or she was entitled to access." *Id.* at *9.

Unlike *Orbit One Communications, Inc.* and the additional cases relied upon by Defendants, Aon does not allege acts that merely constitute trade secret misappropriation. In addition, Aon alleges computer hacking involving file deletions, alterations, accessing files that the Defendants never should have accessed in the first place, and other acts which take this case outside of the more limited allegations faced by Judge Kaplan.

Nor does the First Amended Complaint suffer from the deficiencies found in *Jet One Group, Inc. v. Halycon Jet Holdings, Inc.*, No. 08-CV-3980 (JS)(ETB), 2009 WL 2524864 (E.D.N.Y. Aug. 14, 2009). (Opening Br. at 5, 7, 8, 12.) In *Jet One Group*, Judge Seybert dismissed the CFAA claim there because, among other reasons, the "Plaintiff's opposition papers do not describe the 'extent' to which Hader had access to Jet One's client list, and the Complaint itself places no qualifications on Hader's access." *Id.* at *5. That is not the case here. The First Amended Complaint here alleges that Aon restricted access to client lists and other Aon confidential information stored electronically by "communicating policies to its employees that prohibit the use or disclosure of Aon trade secrets for non-business policies," "restricting access to offices which house such documents," password protecting computer access to only Aon employees, and permitting its employees to use such information "only for legitimate

business purposes in the interest of Aon," and "for the limited purpose of servicing existing business, or developing additional business, for the benefit of Aon, along with other incidental use necessary for their employment with Aon." (FAC ¶¶ 22, 37, 66.)

**B. The First Amended Complaint Pleads A "Loss" Within The Meaning Of The CFAA.**

Defendants' "alternative" argument for dismissal is that Aon did not adequately plead a loss with in the meaning of the CFAA. (Opening Br. at 1, 12-15.) This argument is specious. The CFAA requires a threshold "loss" of at least $5,000 spent on "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of services." *Id.* § 1030(e)(11); *see also EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 584-85 (1st Cir. 2001) (awarding costs of assessing damage); *United States v. Middleton*, 231 F.2d 1207, 1213-14 (9th Cir. 2000) (awarding costs of "investigating and repairing the damage"). In the employer-employee context, the Northern District of New York recently upheld a CFAA claim similar to this one, finding that "[b]ecause Plaintiff has alleged that Defendant's unauthorized activity resulted in over $5,000 in losses, which included the cost to investigate Defendant's actions and assess the resulting damages, Plaintiff has adequately alleged loss sufficient to withstand Defendant's motion to dismiss the CFAA claim." *Penrose Computer MarketGroup, Inc. v. Camin*, 682 F. Supp. 2d 202, 208 (N.D.N.Y. 2010). This is precisely what is pled here.

Defendants cite to *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468 (S.D.N.Y. 2004), *affirmed* 166 Fed. Appx. 559, 562-63 (2d Cir. 2006) for their strained

argument that the First Amended Complaint in this action does not state a claim. The *Nexans Wires* case actually supports Aon's pleading. In *Nexans Wires*, Judge Cederbaum granted summary judgment in favor of defendants on a CFAA claim, ruling that "***travel expenses*** incurred to attend a meeting with [plaintiff's] customers' senior executive, in which no computers are said to have been examined, and no computer consultant said to have been present cannot satisfy the $5,000 'loss' requirement of the statute." *Id.* at 477 (emphasis added). This may be true but it has nothing to do with the allegations in this case. Aon's allegations are far more specific, and definitely related to expenses incurred as a result of Defendants' computer hacking. It is clear that had the plaintiffs in *Nexans Wires* pled their damages as Aon did here, the court would have viewed the pleading differently:

> However, the affidavits do not allege any facts showing that this assessment or response was in any way related to a computer. … It is clear that these meetings were held to discuss the problem of the information of AEA and ASW getting into the hands of competitors. However, nothing suggests that the trips were taken to engage in any type of computer investigation or repair. … In the related action, … [plaintiff does] not allege that they were required to contribute to [costs in investigating the unauthorized access and in making repairs], ***nor do they state that they paid technicians to conduct a computer investigation*** or make repairs to AEB's computers.

*Id.* at 476 (emphasis added).

The First Amended Complaint here pleads what was missing in *Nexans Wires.* Paragraph 48 alleges that Aon hired a forensic consultant, Huron Consulting Group, Inc. "to conduct a computer forensic analysis on the laptops assigned to the Former Employee Defendants while they still worked for Aon, ***to conduct a damage assessment and to restore any data or information that the Former Employee Defendants altered and/or***

***deleted without authorization.***" (FAC ¶ 48, emphasis added). And again, in paragraph 69, Aon alleges losses that exceed $5,000, "which include, without limitation, the costs of investigating defendants' actions, assessing the resulting damages, restoring the data and information altered and/or deleted by the Former Employee Defendants, as well as the costs associated with the interruption to Aon's business[.]" (FAC ¶ 69.) By the plain terms of the CFAA, even as interpreted by *Nexans Wires*, the First Amended Complaint adequately pleads the requisite loss necessary to state a claim. Defendants' position is without merit.

## IV.
## CONCLUSION

Based on the foregoing authorities, Aon respectfully requests that the Court deny this motion to dismiss.

Dated: New York, New York
June 11, 2010

DLA PIPER LLP (US)

By: __/s/ *Robert Johnston*_____

Shand S. Stephens, Esq.
Eliot Kirshnitz, Esq.
Robert A. Johnston, Jr., Esq.

1251 Avenue of the Americas
New York, New York 10020
Tel.: (212) 335-4500
Fax: (212) 335-4501

*Attorneys for Plaintiff*

WEST\22051892.2